CMM
F. #2023R00474

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF (1) ONE PURPLE IPHONE 14 PRO MAX, MODEL NUMBER A2651 ("SUBJECT DEVICE 1"), AND (2) ONE WHITE APPLE IPHONE 12 PRO, MODEL A2341, SERIAL NUMBER G6TFN4MA0D81, IMEI 355103315456742, IMEI2 355103315424930 ("SUBJECT DEVICE 2"), CURRENTLY LOCATED IN THE EASTERN DISTRICT OF NEW YORK	**APPLICATION FOR A SEARCH WARRANT FOR ELECTRONIC DEVICES** Case No. 2:23-MJ-01032 (JMW)

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, WILLIAM SENA, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been a Special Agent with the FBI for approximately seven years. As an FBI Special Agent, I conduct investigations into, among other things, bank fraud, mail and wire fraud and other

economic crimes. During my tenure with the FBI, I have participated in numerous financial fraud investigations and have participated in all aspects of investigations, including conducting surveillance, executing search warrants, debriefing defendants and informants, interviewing witnesses, reviewing and analyzing recorded conversations and analyzing toll information. During the course of these investigations, I have served as the lead investigator in the investigation and prosecution of persons involved in various financial frauds, among other crimes. I am aware that criminals engaging in financial fraud commonly use electronic means of communication in furtherance of their criminal activities, including but not limited to text message, instant message and electronic mail. As a result of my training and experience, I am familiar with techniques and methods of operation used by individuals involved in criminal activity to facilitate various kinds of frauds and to conceal their activities from detection by law enforcement authorities.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: (a) my personal participation in this investigation; (b) reports made to me by other law enforcement officers; and (c) review of bank records, toll records and other records and reports. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1343 and 1344 (wire and bank fraud) and 18 U.S.C. §§ 2 and 1349 (aiding and abetting and conspiracy to commit wire and bank fraud) (collectively, the "Subject Offenses") have been committed. There is also probable cause

to search the information described in Attachment A for evidence and instrumentalities of these crimes as described in Attachment B.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is (1) one purple iPhone 14 Pro Max, Model Number A2651 ("SUBJECT DEVICE 1") and (2) one white Apple iPhone 12 Pro, Model A2341, Serial Number G6TFN4MA0D81, IMEI 355103315456742, IMEI2 355103315424930 ("SUBJECT DEVICE 2") (collectively, the "SUBJECT DEVICES"). The SUBJECT DEVICES are currently located in the Eastern District of New York.

6. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On November 8, 2023, a grand jury sitting in the Eastern District of New York returned an indictment charging JORGE ARIAS, NELSON BAYONA, OSCAR BAYONA JR., also known as "Oscar Suarez," JAMES CABAN and ESPERANZA ORTIZ (collectively, the "defendants") with the Subject Offenses. See 23-CR-456 (JMA) (the "Indictment"). A copy of the Indictment is attached hereto as Exhibit A and incorporated by reference herein.

8. By way of background, the FBI has been conducting a criminal investigation of the defendants, and others known and unknown, for possible violations of the Subject Offenses.

9. In particular, and as set forth in the Indictment, from approximately September 2019 to the present, the defendants each applied for and received, or attempted to receive, loans, lines of credit ("LOC") and/or credit cards from various financial institutions throughout the United States, including within the Eastern District of New York. Much of the underlying documentation contained materially false information, including about the defendants' residence, employment and income, that made the defendants falsely appear more creditworthy. For example, the applications falsely stated that the defendants were employed by particular businesses and included grossly inflated incomes for the defendants. In addition, the defendants submitted fraudulent supporting documentation, including, but not limited to, fake paystubs and fake driver's licenses as part of the applications.

10. As a result of this fraudulent conduct, the financial institutions approved the applications that contained materially false and fraudulent information and disbursed loans and LOCs and issued credit cards to the defendants.

11. After receiving and exhausting the loan, LOC or credit limit, the defendants paid the loan, LOC or credit card, using checks from accounts with insufficient funds. By the time the checks were returned for insufficient funds, the defendants had already withdrawn additional funds made available from paying the loan, LOC or credit card, causing the financial institutions to incur additional losses. The below sets forth examples of this fraud scheme with respect to one financial institution, which is identified in the Indictment as Credit Union-1.

O. BAYONA

12. On March 17, 2022, O. BAYONA applied for a LOC from Credit Union-1. On his loan application, O. BAYONA stated that he had been employed as a Regional Manager at

SNM Movers for approximately three years, with a monthly income of approximately $11,666. He also provided a New Jersey driver's license for purposes of identification.[1] Based on this false information, Credit Union-1 approved O. BAYONA for a $50,000 LOC.

13. Between March 17, 2022 and March 31, 2022, O. BAYONA withdrew $30,005 from the LOC in the form of two cashier's checks made payable to himself.

14. On August 15, 2022, O. BAYONA made two $25,000 payments to the Credit Union-1 LOC through Billmatrix.[2] The next day, on August 16, 2022, he withdrew $25,000 from the LOC at Jovia in Franklin Square, New York, and then another $25,000 at Jovia in New Hyde Park, New York.[3]

15. Ultimately, both $25,000 payments to the Credit Unin-1 LOC made through Billmatrix were returned for insufficient funds. As a result, the amount due on O. BAYONA's Credit Union-1 LOC was approximately $99,780.

CABAN

16. On April 7, 2022, CABAN opened a checking and savings accounts with Credit Union-1. That same day, he applied for a $50,000 LOC. On his loan application, CABAN stated that he had been employed as a Regional Manager at SNM Movers for approximately four

---

[1] A review of law enforcement databases reveals that the State of New Jersey has not issued O. BAYONA a driver's license.

[2] Billmatrix provides electronic bill payment services for companies in the financial services industries, among others.

[3] These are examples of a shared branch transaction. In a shared branch network, a credit union's members can go to branches of other credit unions in the network and conduct transactions as they would at their own credit union.

years, with a monthly income of approximately $11,152. He provided ADP paystubs from "SNM Movers" as proof of income.[4] He was approved for a $20,000 LOC, and he immediately withdrew the full $20,000.

17. On April 22, 2022, CABAN applied for a Visa credit card through Credit Union-1 with the same identifying information that he used on the LOC application. He was approved the same day for a $30,000 credit limit. That same day, April 22, 2022, he took a $20,000 cash advance from the Credit Union-1Visa credit card and deposited the $20,000 into his Credit Union-1 checking account.

18. On April 23, 2022, CABAN withdrew the $20,000 from the Credit Union-1 checking account at Jovia in Rockville Centre, New York in the form of a teller's check made payable to himself.

19. On May 4, 2022, CABAN took a $10,000 cash advance from the Credit Union-1 Visa credit card and deposited it into his Credit Union-1 checking account. That same day, he withdrew $400 from the checking account and made a $400 payment to the LOC. The next day, May 5, 2022, he made a $9,500 over-the-phone payment to Discover from the checking account.

20. On July 5, 2022, CABAN made two payments to the credit card: (i) a $25,000 payment; and (ii) a $5,002 payment. On the same day, he took a $29,700 cash advance from the credit card and deposited the money into his Credit Union-1 checking account. He immediately withdrew $27,000 from the checking account in the form of (i) a $25,000 check made

[4] ADP confirmed that the alleged employer was not an ADP client.

payable to himself at Jovia in Rockville Centre, New York, and (ii) $2,000 in cash at the BFCU in Freeport, New York.

21. On July 12, 2022, CABAN made two payments to the credit card: (i) a $24,000 payment and (ii) a $5,997 payment. He also made a $20,261.02 payment to the LOC.

22. The next day, July 13, 2022, CABAN took a $30,000 cash advance from the credit card and deposited it into the checking account. Once the funds transferred, he withdrew $25,000 from Jovia in Valley Stream, New York, and $4,000 from Jovia in Rockville Centre, New York, both in the form of a teller's check made payable to himself.

23. On July 14, 2022, CABAN transferred $20,000 from the LOC (the balance that was made available from the July 12 payment) to the checking account. After a few transactions that same day, the checking account was left with a balance of $19,319.

24. Ultimately the $25,000, $5,002, $24,000, and $5,997 payments (from July 5 and July 12) made to the credit card were reversed for insufficient funds. The $20,261.02 payment (from July 12) to the LOC was also returned for insufficient funds. On March 20, 2023, after months of inactivity, Credit Union-1 transferred the $19,319 balance that was left in the checking account to the outstanding LOC. Credit Union-1 was left with a loss of $20,036.05 on the LOC and $89,578 on the credit card, for a total of $109,614.05.

N. BAYONA

25. On May 27, 2022, N. BAYONA applied for a LOC from Credit Union-1. On his membership application, he identified the call number assigned to SUBJECT DEVICE 2 as his cellphone number. He also stated that he had been employed as a Supervisor at SNM Movers for approximately five years, with a monthly income of approximately $12,333.33. Based on this

false information, Credit Union-1 approved N. BAYONA for a $50,000 LOC. That same day, he immediately exhausted the full amount of the LOC by withdrawing $50,000.

26. On June 30, 2022, N. BAYONA paid the LOC in full via two $25,000 payments made through Billmatrix. The next day, on July 1, 2022, he withdrew $25,000 from Jovia in Valley Stream, New York, and $24,500 from Jovia in Rockville Centre, New York.

27. Ultimately, both payments made through Billmatrix were returned for insufficient funds. As a result, the amount due on N. BAYONA's Credit Union-1 LOC was approximately $99,500.

ORTIZ

28. On May 27, 2022, ORTIZ applied for a LOC from Credit Union-1. On her application, she stated that she was employed as a Regional Manager at Landy's International for approximately 7 years, with a monthly gross income of approximately $12,499.50. She provided Paylocity paystubs from Landy's Hair Products Corp. as proof of income.[5] Based on this false information, Credit Union-1 approved ORTIZ for a $50,000 LOC.

29. ORTIZ immediately exhausted the full amount of the loan by transferring $50,000 to her Credit Union-1 savings account. That same day, on May 27, 2022, she (i) withdrew $35,000 from her Credit Union-1 savings account, (ii) transferred $15,000 from her Credit Union-1 savings account to her Credit Union-1 checking account, and (iii) deposited $10,000 into her Credit Union-1 checking account. Four days later, on May 31, 2022, she withdrew $25,000 from her Credit Union-1 checking account via check made payable to herself.

[5] Paylocity confirmed that the alleged employer was not a Paylocity client.

30. On June 30, 2022, ORTIZ made a $44,598.84 payment to the Credit Union-1 LOC with a check drawn from her MCU Account ending in 5111 (the "MCU 5111 Account")[6] at Ocean Financial in Seaford, New York.

31. On that same day, June 30, 2022, ORTIZ applied for and obtained a $30,000 LOC from Credit Union-1. The next day, on July 1, 2022, she exhausted this second Credit Union-1 LOC; specifically, she withdrew $25,000 from the LOC at Jovia in Uniondale, New York, and $5,000 from the LOC at BFCU in Hempstead, New York.

32. On July 21, 2022, ORTIZ paid the LOC in full with a $30,000 check drawn on the MCU 5111 Account[7] at Ocean Financial in Seaford, New York. Again, she immediately exhausted the LOC. That same day, she withdrew: (i) $25,000 from the LOC at Jovia in Valley Stream, New York, (ii) $2,000 from the LOC at BFCU in Freeport, New York, and (iii) $2,000 from the LOC at Western Union in Freeport, New York.

33. Ultimately, all payments made by ORTZ to Credit Union-1 for both LOCs were returned for insufficient funds. As a result, the amount due on ORTIZ's two Credit Union-1 LOCs was approximately $109,000.

ARIAS

34. On October 12, 2022, ARIAS applied for a LOC from Credit Union-1. On his application, he stated that he was employed as a Marketing Director at Splexknow Corp., earning a monthly income of approximately $14,191.67. He provided ADP paystubs from

[6] The MCU 5111 Account had a balance of $550 when the check was used.

[7] The MCU 5111 Account had a balance of $340 when the check was used.

Splexknow Corp. as proof of income.[8] Based on this false information, Credit Union-1 approved ARIAS for a $15,000 LOC. He immediately transferred the $15,000 LOC funds to his checking account.

35. On October 15, 2022, ARIAS withdrew $15,000 from his Credit Union-1 checking account at Jovia in Franklin Square, New York.

36. On November 2, 2022, ARIAS made a $15,029.70 payment to the LOC. The following day, November 3, 2022, he withdrew $15,000 from the LOC at Jovia in Hempstead, New York.

37. On November 4, 2022, ARIAS made a $13,500 payment to the LOC at Ocean Financial in Seaford, New York. He immediately withdrew $13,500 from the LOC by transferring it to his Credit Union savings account. He then withdrew the funds at Jovia in Wantagh, New York.

38. Ultimately, both the November 2 payment of $15,029.70 and the November 4 payment of $13,500 were returned for insufficient funds, leaving Credit Union-1 with a loss of $43,417.98.

39. On October 27, 2022, ARIAS applied for a Visa credit card through Credit Union-1; he used the same identifying information as the LOC application. Credit Union-1 approved him for a credit card with a $10,000 limit.

40. On October 31, 2022, ARIAS took a $10,000 cash advance from the credit card.

[8] ADP confirmed that the alleged employer was not an ADP client.

41. On November 2, 2022, ARIAS made a $10,100 payment to the credit card.

42. The following day, November 3, 2022, ARIAS took a $10,000 cash advance from the credit card. The next day, November 4, 2022, he made a $10,100 payment to the credit card. That same day, November 4, he took another $10,000 cash advance from the credit card.

43. Ultimately, both the $10,100 payments (from November 2 and November 4) were reversed for insufficient funds, leaving Credit Union-1 with a loss of $30,000 on the credit card.

THE SUBJECT DEVICES

44. On November 8, 2023, law enforcement officers arrested O. BAYONA at John F. Kennedy International Airport in Queens, New York, pursuant to an arrest warrant following the Indictment. O. BAYONA was in possession of SUBJECT DEVICE 1 at the time of his arrest. Law enforcement officers took custody of SUBJECT DEVICE 1 at that time.

45. On November 9, 2023, law enforcement officers arrested N. BAYONA in Championsgate, Florida, pursuant to an arrest warrant following the Indictment. N. BAYONA was in possession of SUBJECT DEVICE 2 at the time of his arrest. Law enforcement officers took custody of SUBJECT DEVICE 2 at that time. SUBJECT DEVICE 2, which is in FBI custody, was transferred from the Middle District of Florida to the Eastern District of New York.

46. Therefore, while the FBI might already have all necessary authority to examine the SUBJECT DEVICES, I seek this additional warrant out of an abundance of caution to be certain that an examination of the SUBJECT DEVICES will comply with the Fourth Amendment and other applicable laws.

47. Based on the above, there is probable cause to believe that the defendants, including, but not limited to, O. BAYONA and N. BAYONA, and others whose identities are known and unknown, were involved in the Subject Offenses. Further, there is probable cause to believe that information on the SUBJECT DEVICES will produce evidence probative of the crimes under investigation.

48. Based on my training and experience, I know that individuals who engage in bank and wire fraud commonly use mobile devices such as cellular telephones to communicate with co-conspirators through voice calls, text messages, instant messages, emails and other means. I further know that individuals who commit bank and wire fraud often use mobile devices to arrange and plan the execution of the crimes.

49. The SUBJECT DEVICE 1 is currently in the lawful possession of the FBI after being recovered from O. BAYONA incident to his lawful arrest; and SUBJECT DEVICE 2 is currently in the lawful possession of the FBI after being recovered from N. BAYONA incident to his lawful arrest.

50. The SUBJECT DEVICES are currently located in the Eastern District of New York. In my training and experience, I know that the SUBJECT DEVICES have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICES first came into the possession of the FBI.

TECHNICAL TERMS

51. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

52. Based on my training, experience, and research, I know that the SUBJECT DEVICES have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, PDAs and GPS navigation devices. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT DEVICES.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

53. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

54. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose(s) of each's use, who used each device, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

55. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the SUBJECT DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

56. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

57. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICES described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

William Sena
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on November 17, 2023:

IN person @ 1:56 pm

/S/ James M. Wicks by ~~FACETIME~~

HONORABLE JAMES M. WICKS
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is (1) one purple iPhone 14 Pro Max, Model Number A2651 ("SUBJECT DEVICE 1") and (2) one white Apple iPhone 12 Pro, Model A2341, Serial Number G6TFN4MA0D81, IMEI 355103315456742, IMEI2 355103315424930 ("SUBJECT DEVICE 2") (collectively, the "SUBJECT DEVICES"). The SUBJECT DEVICES are currently located in the Eastern District of New York.

This warrant authorizes the forensic examination of the SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the SUBJECT DEVICES described in Attachment A that relate to violations of 18 U.S.C. §§ 1343 and 1344 (wire and bank fraud) and 18 U.S.C. §§ 2 and 1349 (aiding and abetting and conspiracy to commit wire and bank fraud) (collectively, the "Subject Offenses") and involve Oscar Bayona, Jr., also known as "Oscar Suarez," and Nelson Bayona and their co-conspirators, including, but not limited to:

   a. names and telephone numbers, as well as the contents of all call logs, contact lists, text messages (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Instagram posts, Internet activity (including browser history, web page logs, and search terms entered by the user), geo-location data, application data, and other electronic media;

   b. lists of financial institutions and related identifying information;

   c. all bank/financial institution records, checks, credit card bills, account information, and other financial records, including but not limited to, membership applications, and loan, lines of credit and credit card applications, as well as dates, places, and amounts of specific transactions at financial institutions; and

   d. any information recording O. BAYONA's, N. BAYONA's or co-conspirator's schedule or travel.

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet Protocol addresses to communicate with various financial institutions, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. Evidence of software that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

5. Evidence of the times the SUBJECT DEVICES were used;

6. Password, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICES; and

7. Contextual information necessary to understand the evidence described in this Attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigative agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.